A Research Proposal

on

Fortification of Transport Layer Security Protocol by generating an Ideal Password Authentication Scheme

Submitted to

LOVELY PROFESSIONAL UNIVERSITY

in partial fulfillment of the requirements for the award of degree of

DOCTOR OF PHILOSOPHY (Ph.D.) IN (Computer Applications & Information Technology)

Submitted by:	**Supervised by:**
Kuljeet Kaur	Dr.G.Geetha

LOVELY FACULTY OF TECHNOLOGY AND SCIENCES
LOVELY PROFESSIONAL UNIVERSITY
PUNJAB

1. Introduction

Whenever there is communication between Client and Server over a public link and resources are to be accessed from remote systems, then proving an identity becomes quiet complex because there is need of proper access rights with authentication. The most convenient mechanism to prove authenticity over public link to access from remote systems is the use of Password. So over a public network, communication could be started by sharing a (short) password within a session created between Client and Server with Session key. For this, Secure Shell protocol (SSP) is deployed [1]. Public Network is an insecure network so Password authentication is one of the simplest and the most convenient authentication mechanisms to deal with secret data over this insecure network. Password Authentication is required in areas such as wireless networks, remote login systems, and DBMS etc [2].

Example: Whenever user wants to access Online Banking, they require an identifier (ID) and password (PW). The user enters the ID and PW on the login screen, and then server verifies the same ID and PW in the Password (verification) table. If the submitted ID and PW match with the server's password table, the user will be granted access to the server. Here Public Key Infrastructure (PKI) is used where server knows the secret key corresponding to the public key embedded in a certificate of security.

But there is a possibility that an intruder can impersonate a legal user by stealing the user's ID and PW from the password table. Moreover intruder can make use of various attacks (Dictionary Attack, Denial of Service, Man in the Middle Attack etc) during communication of the data and could possibly impersonate the legal user. All these attacks and impersonation is possible only on the transport layer because when the data is being transferred security protocols could be broken by the intruders and they could hack the password.

i. In SSP the client is asked to log into another computer at some remote location but with some password authentication, then only files could move from one location to another. Remote Machine maintains association between client name and password.

ii. In Public Key Infrastructure, the password authenticated key exchange provides two computing devices with session key to implement an authenticated communication channel within which messages sent over the wire are cryptographically protected.

But in both the protocols security of the password becomes the prime concern for every data communication over the public network.

Presently there are various password authentication schemes which are being used by organizations as a bolster to password when communicating over the public network. Current data security and cryptographic techniques or schemes for password authentication are:

1. RSA based
2. ElGamal based
3. Hash based

Intruders try various attacks such as denial of service attacks, forgery attacks, forward secrecy, and server spoofing attacks, password guessing attacks, replay attacks, and smart card loss attacks and could not withstand the security requirements such as DNS poisoning, forward secrecy, mutual authentication and ping broadcast etc on these schemes.

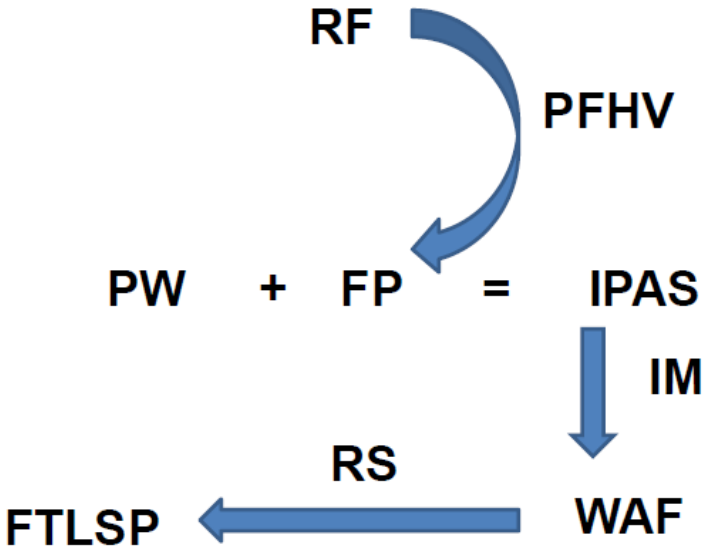
Organizations are using SSL (Secured Socket Layer) in their Virtual Private Networks (VPN) (which is created virtually over a public insecure network) for securing end to end transport [2]. This protocol has various advantages like it provides a secure connection between remote users and internal network resources, it has outbound connection security and it does not require additional client software to be installed on the end point device. This protocol seems secure but there are a number of risks which lurk in its use. e.g [3] Lack of required host security software on public machines, Physical access to shared machines, Keystroke loggers, Endpoints—loss of sensitive information and intellectual property, Man-in-the-middle attacks etc. CISCO have identified that security of the data at Transport Layer with SSL [3] could only be possible if following statements are implemented:

1. Security policies and secure access through strong user authentication
2. Host identity verification
3. Host security posture validation
4. Secure desktop
5. Cache cleaning
6. Keystroke logger detection
7. Configuration consideration
8. User education and security awareness

But the complete security starts with proof of authentication, which is done by passwords in majority of the organizations which are not that secure. A Survey should be done to identify the most acceptable identity authentication parameter (Smart Card, Fingerprint, Iris, Voice Recognition and Pass Phrase etc). Combination of different identity authentication parameters should be used to generate an Ideal Password Authentication Scheme (IPAS).If authentication process could be in tiers with the help of IPAS then it would make the data transfer or communication process more secure. Application of the IPAS would result in the fortification of the transport layer security protocol. In this research proposal password would be assimilated with the finger print for generating IPAS which would be having new fingerprint hash algorithm implemented and when applied would result in enhancement of security the transport layer on the public network.

The existing password authentication schemes (RSA, ElGamal and Hash) fail to withstand all the security requirements (Evidence of this is shown in the *Figure 1*). In majority of the organizations Hash Based Scheme is used because it is vulnerable to smart card loss attack only but could withstand the security requirement of mutual authentication. Mutual Authentication means proof of authenticity or identity authentication at both the ends (Client and Server) for which finger prints are combined with passwords. One more tier to the security protocol would be added by combining finger print to the password for generating IPAS. This IPAS would be applied to transport layer for proving its resourcefulness. After adding one more tier to the security protocol by adding finger prints, requirement of hash algorithm would generate. Proposal would result in generation of new fingerprint hash algorithm (RNA-FINNT). User's fingerprint would be taken as identification and RNA-FINNT would change the finger print value into the hash code and store the same value to the database. Every time when user would put finger as identification a new hash code value would be generated because location of the fingerprint could not be fixed, so then transformations would be done with the produced hash code which would ultimately be matched with the already stored hash value of the fingerprint. If this value matches then it proves the user's authenticity. So process for generating an IPAS with the proof of its application resulting in fortification of Transport Layer Security Protocol is as follows:

Password = PW
Fingerprint = FP
RNA-FINNT = RF
Process of Extracting Fingerprint Hash Value = PFHV
Implementation = IM
Ideal Password Authentication Scheme = IPAS
Result = RS
Web Application Framework =WAF
Fortification of Transport Layer Security Protocol = FTLSP



Process 1: Process for generating IPAS with proof of Implementation resulting in FTLSP

There are various hash algorithms available but this research proposal would generate a new hash algorithm (RNA-FINNT) which would work more efficiently, would take less time in calculation and faster than the existing hash algorithms. This new hash algorithm would take finger print as input and hash code as output, the value of which would be stored at the Server. The password and finger print together would be used for proving mutual authentication and the application of IPAS (*Process 1*) would result in fortification of TLSP.

Mutual authentication in the Multi Server Environment (MSE) of an organization is required in application of IPAS so that intruders could not practice IP or Server Spoofing etc. Phishing would be extremely difficult if mutual authentication is implemented well in IPAS.

So this research proposal would use password and fingerprints for identity authentication (Ideal Password Authentication Scheme (IPAS)) of Client and Server both (Mutual Authentication) which would result in the Fortification of Transport Layer Security Protocol (FTLSP). And this Ideal Password Authentication Scheme (IPAS) could be implemented in any organization with multi-server environment (MSE).

2. Review of Literature

Users make use of passwords over a network for security. And in organizations SSL Protocol is implemented in their VPN for security of data at Transport Layer. But intruders perform various attacks for hacking the passwords. So users are regularly being instructed not to share their password and are advised to generate strong passwords. Users generate strong passwords and at the back end password authentication schemes work for security and strength of the password. But these schemes are vulnerable to various attacks which results in insecurity. Let us first discuss kind of attacks, for which scheme should not be vulnerable, and security requirements, which scheme should satisfy. In this research proposal certain security requirements and attacks along with their brief description are finalized which are mandatory for all the password authentication schemes to withstand:

1. **Denial of Service Attack**[4]

   The goal of this attack is to deny legitimate users access to particular resources. False verification information of the legal user can be updated by the attacker for the next login phase. Later on the legal user would not be able to login successfully. A malicious user intentionally disrupts service to a computer or network resource.

2. **DNS Poisoning**[5]

   A computer sends a question to the DNS Server and gets an answer and if the answer appears to match the question it asked, computer completely trusts that the name server is correct and start transmitting data. Traffic on the internet can be intercepted, rerouted or impersonated so that the answer given by the legal server proves to be false.

3. **Forgery Attack**[6]

   It is a kind of impersonation attack in which an attacker attempts to modify intercepted communications to masquerade the legal user and login the system to access the resources at the remote system. Remote user authentication is very important for security of systems which allows remote access over public (untrusted) network, on which forgery attacks become quite common.

4. **Man in the Middle Attack**[7]

   In this an attacker intercepts (views or modifies) sensitive data sent to or received by a user from the router in an untrusted public network, by deploying injections, key manipulations and filtering etc. This attack is possible when different clients share the same secret or the intruder could generate fake security certificate or the attacker is able to modify the payload of the packets by recalculating the checksum etc.

5. **Forward Secrecy**[8]

   This is the security requirement that ensures that the previously generated passwords in the system are secure even if the system's secret key has been revealed in the public by accident or is stolen. Key once used for transmission of data should not be used to derive any new key. But if the key is derived from some other material then that material should not be used to derive any more keys.

6. **Ping of Death**[9]

   It is a type of attack in which malicious ping is sent to a computer. Attacker only needs to know the IP address of the machine which it has to attack, no other information is required. Attacker sends the oversized packet because the attacker need not to know anything about the machine which it is attacking except IP address so spoofing of attacker becomes easy. So an illegal echo packet with more bytes than allowed is sent, it results in buffer overflow, crashes and data fragmentation etc.

7. **Mutual Authentication**[10]

   In this the user and the server can authenticate each other. This means not only the server verifies the legitimate user but the user also verifies the legitimate server. This security requirement helps to withstand server spoofing.

8. **IP Spoofing**[11][12]

   This is basically lying about an IP address. In this the source address given is normally incorrect. So when the source address is not true then it lets an attacker assume a new identity because the source address is not the same as the attacker's address, so any replies generated by the destination would be sent to the attacker. And if the attackers adhere to the protocol requirements then the connection would be very well maintained. IP Spoofing exploits trust relationships between routers.

9. **Parallel Session Attack**[13]

   When user and server communicate with each other, an attacker could create a valid login message out of some eavesdropped communication of the user and the server. For this attacker need not to know the user's password, one could easily masquerade legitimate user by creating a valid login. It occurs when two or more protocol runs are executed concurrently and messages, from one run (the reference session) are used to form spoofed messages in another run (the attack session).

10. **Ping Broadcast**[14]

    If there is large number of hosts then a ping request packet is sent to the network to all the hosts. IP address of the machine which is to be attacked is mentioned in the source address. Now when request is sent to the network then all the hosts reply to the ping to the attacked system. So the attacked machine would be flooded with ping responses which will result that the attacked machine would be unable to operate or even this may result in locking of the attacked machine.

11. **Password Guessing Attack**[15]

    In this attacker intercepts the authentication messages and stores them locally and then attempts are continuously made to guess password. Majority passwords have very low entropy and are very vulnerable to password guessing attacks. Attacker verifies the correctness of guess by using these authentication messages.

12. **Server Spoofing**[16]

    In this attacker pretends to be server to manipulate sensitive data of the legitimate users. The attacker creates a situation to masquerade legitimate user by falsifying data and getting an access as legitimate user. It generally happens because TCP/IP does not provide any mechanism by which authentication of source or destination message could be proved. Because of this data becomes vulnerable to server spoofing attack.

13. **Replay Attack**[17]

    An attacker saves the previous communications of the legitimate user. Attacker intercepts the previous communications and can easily impersonate the legitimate user in order to login into the system. The attacker can replay all these intercepted messages and it would result in impersonation of legitimate user. This attack involves

capturing traffic and uses that to gain access to the systems. e.g Login information of the valid user is sniffed by the hacker. Now even if the information is encrypted, the hacker replays the login information and gains the access.

14. **Session Hijacking**[18]

    In this attack the attacker directs traffic to its own server rather than routing that to trusted server. In order to hijack a session, the hacker ARP poisons (Address Resolution Protocol Poisoning means that the ARP communication is intercepted by redirection from a router) the router so that all traffic is routed to attackers computer before it is delivered to the trusted server. Session hijacking is host based and network based. Because of session hijacking attacker can inject data into an unencrypted server to server traffic, client to server traffic, hide origin of the malicious attacks and denial of service attacks could be easily performed.

15. **Smart Card Loss Attack**[19]

    If the smart card of the legitimate user is lost or stolen the attacker can easily change the password of the smart card by using password guessing attacks, dictionary attacks and could impersonate the legitimate user in order to login into the system.

16. **Smurf Attack**[20]

    It is a DOS attack but not operating system specific; in this the target network generates large number of PING requests with spoofed IP addresses. Each PING request is broadcast which results in large number of responses flooded from all the nodes on the network. So it prevents legitimate requests from being processed.

17. **Stolen Verifier Attack**[21]

    The passwords are stored in the hashed code at the server. In this attack the attacker steals the passwords (hashed code) from the server and can easily impersonate the legitimate user to login into the system. Hashed code stolen is used by attacker as stolen verifier for impersonating legitimate user.

18. **Teardrop Attack**[22]

    It is a kind of denial of service attack which exploits the way that the Internet Protocol (IP) requires a packet that is too large. Now as the packet is large so the router could not handle it and there is need to divide the packet into fragments. In this

attack the attackers IP puts a confusing offset value in the second or later fragment. If the receiving operating system could not handle this problem then it could result in system crash.

According to this research proposal above said are the attacks and security requirements which are generally being practiced by intruders. The existing password authentication schemes are vulnerable to various above said attacks and could not withstand majority of the above said security requirements. At the transport layer these existing schemes along with various security protocols, sometimes are unable to safeguard communication process. For proof of this let us first discuss the existing password authentication schemes along with their processing and verify, that the said scheme is vulnerable to which attack and could not withstand which security requirement.

Below mentioned are the existing password authentication schemes:

1. **RSA Based Scheme**[23]

   This is public key cryptosystem which was proposed by Rivest, Shamir and Adleman in 1978. It is used for encryption. Its security is based on factoring large or huge numbers.

   Process followed in this scheme is [23]:

   i. Take two prime numbers *p* and *q*, multiply them and compute *N*.
   ii. Now *p* and *q* are the private keys used and the *N* is public key. It is very easy to compute public key i.e *N* but it is very difficult to calculate the private key because lot many factor multiplications are required for assuming *p* and *q*.
   iii. Choose one relative prime number *e* (Public Key) by calculating *(p-1) (q-1)*.
   iv. On the basis of Chinese Remainder Theorem compute *c* by M^e *(mod N)*. Now this *c* is the encoding which is sent by *B* to *A*.
   v. Now if *A* wants to decode the message, calculations would be done on the basis of Fermat's Little Theorem i.e *ed=1(mod (p-1) (q-1))* and c^d *(mod N)*.
   vi. These calculations would result in generating *M*. Now if this generated *M* is same as the send message then authenticity is proved otherwise someone is trying to impersonate the legitimate user.

The scheme very well proves the authenticity of the user with the said algorithm, at the Client and Server end, attacker would fail in any of the step and would be unable to impersonate legitimate user. This scheme uses one way ciphers or trap door ciphers in which key for encoding (public key) is different from key for decoding (private key). **But the scheme is vulnerable to and could not withstand the mutual authentication security requirement.** Security certificate is required because public key could be used to forge a message and it should be changed with each message.

2. **ElGamal Based Scheme**[24]

It is proposed by ElGamal in 1985. It is public key cryptosystem used for encryption. In it discrete logarithms are calculated depending upon the finite numbers. This scheme is an alternative to RSA for public key encryption. As far as RSA is concerned its security lies in factoring large integers, but security of ElGamal algorithm depends on computing discrete logs of large prime numbers.

Process followed in this scheme to check the authenticity is as follows [24]:

i. Choose one prime number q and two random numbers g and x such that both the numbers are smaller than q.

ii. Pick another random number k and compute $p = 2^k q+1$

iii. Compute $y= g^x \bmod q$

iv. x is the private key. p,g *and* y are public key and M is message sent by A to B.

v. In order to perform encryption two calculations would be done i.e
$a = y^k M \bmod p$ and $b = g^k \bmod p$ so output would be (a,b)

vi. Now decryption would be performed that M would be computed that either
$M = a$ *or* $M = b^x$

The scheme very well proves the authenticity of the user with the said algorithm, at the Client and Server end, attacker would fail in any of the step and would be unable to impersonate legitimate user. Semantic security is used in this scheme. This scheme has the advantage that same plaintext gives a different ciphertext every time when it is encrypted but disadvantage with the scheme is that the ciphertext is twice as long as the plaintext. [25] In this scheme different random number has to be chosen every time by the sender and the receiver, whenever they want to communicate, because of

the security protocol at the transport layer. Encryption under this scheme requires exponentiations twice (these exponentiations are independent of message) but decryption only requires one exponentiation.Three steps are followed in this scheme [25]:

i. Setup (generating public and private or secret key)
ii. Encrypt (takes message and public key as input and produces cipher text)
iii. Decrypt (takes cipher text and secret key and produces message).

But the scheme is vulnerable to and could not withstand the mutual authentication security requirement.

3. **Hash Based Scheme**[26]

This scheme uses various types of hashing which would enhance the performance of the transmission. Hashing could be done as follows [26]:

i. One way Hashing (i.e y = h(x))
ii. Direct Hashing (i.e Hashing of source and destination address using XOR gate and performing the checksum of the internet)
iii. Table based Hashing (i.e Separates traffic splitting on the transport layer and load allocation at the transport layer)

While implementing One-way or direct hash scheme, a message with arbitrary length is taken as an input and a fixed length message is produced as an output. To explain this take a function *y* as *y = h(x)* which takes message *x* having arbitrary length as input and returns fixed length hash value *y* as output[26]. When the sender assumes that the message is correct this hash value is appended to the message by the sender at the source and the receiver authenticates the message by recomputing the hash value [27].Process to be followed for hashing is as follows:

i. Take block data of any size and hash scheme *h* would be applied to it.
ii. *h* would take arbitrary length input and would produce a fixed-length output.
iii. It is very easy to compute *h(x)* for any given value of *x*. *(There exists a polynomial-time algorithm that on input x outputs h (x))*
iv. But if *h(x)* is given, it becomes infeasible to find *x*. *(There is negligible probability to find inverse of x under h in polynomial time algorithm)*

v. Even if $h(y) = h(x)$ then also it is computationally infeasible to find that $y \neq x$. It is because of the weak collision resistance at the transport layer. *(With some non-negligible probability, all inverting algorithms fail to invert functions)*

vi. Now even if the transport layer has strong collision resistance it is computationally infeasible to find any pair (x,y) such that $h(x) = h(y)$. *(There is a negligible success in inverting functions by any efficient algorithms)*

Hashing could be done with hashfunction, hashset, hashmap. The said code would be used to encrypt the information to be said. Hashcode always returns same value for the same input, it is consistent method. [28] A good hashcode method is efficient to compute, gives uniform distribution of values (better than RSA and ElGamal) and mathematical analysis is required to prove that the cost of inserting into hash table or searching value in the hash table is O(1). The scheme uses smart card and password for identity verification. **The scheme is vulnerable to smart card loss attack but could very well withstand the requirement of mutual authentication.**

After analyzing the existing schemes conclusion is drawn that hash based scheme is being used by majority of the organizations because it is more convenient to use and more secure than other schemes. But as this scheme is vulnerable to smart card loss attack so following steps would be used in the research proposal:

1. Hashed finger print would be used as a parameter rather than smart card.
2. Mutual authentication would be done; new fingerprint hash algorithm would be used.
3. User name along with middle finger print would be used for Sever side authentication and password along with index finger print would be used for Client side authentication.

Above mentioned steps would help in the overall fortification of the transport layer security protocol.

These existing password authentication schemes use either password or smart card for proving the user's identity over the network for security but from the below said table it is very well verified that these schemes are vulnerable to smart card loss attack and could not withstand mutual authentication security requirements. Comparative analysis of all the

existing password authentication schemes with the security requirements and attacks which it could not satisfy and is vulnerable to:

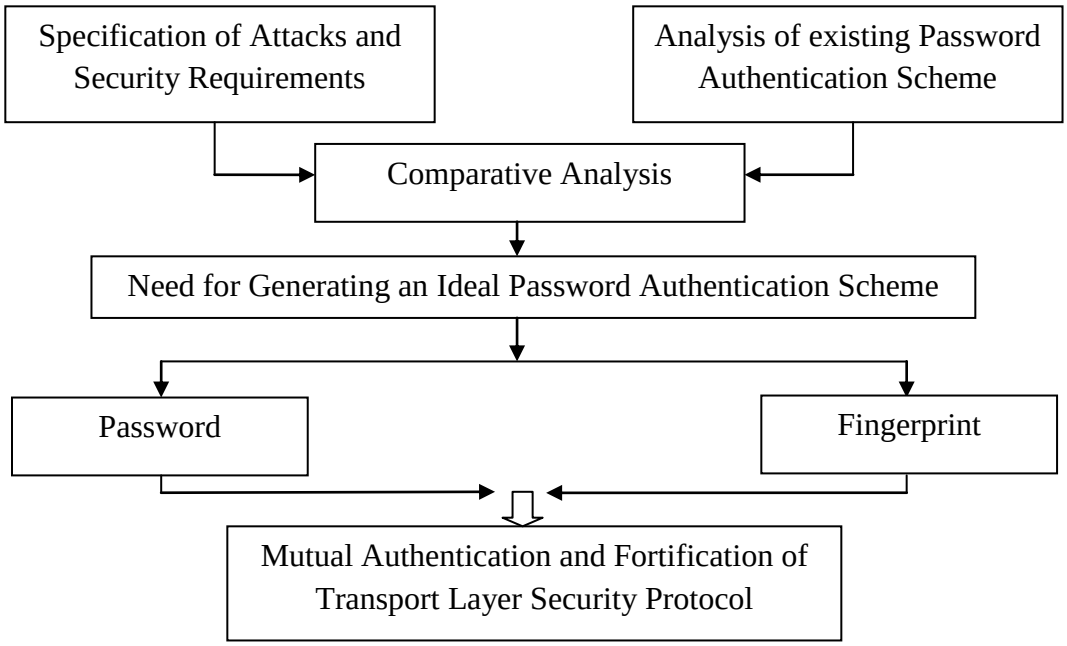
Y: Supported N: Not Supported

S.No	Security Requirements and Attacks	RSA Based Scheme	ElGamal Based Scheme	Hash Based Scheme
1	Denial of Service Attack [4],[23],[24],[26],[27]	Y	Y	Y
2	DNS Poisoning [5], [23],[24],[26],[27]	Y	Y	Y
3	Forgery Attack [6], [23],[24],[26],[27]	Y	Y	Y
4	Man in the Middle Attack [7], [23],[24],[26],[27]	Y	Y	Y
5	Forward Secrecy [8], [23],[24],[26],[27]	Y	Y	Y
6	Ping of Death [9], [23],[24],[26],[27]	Y	Y	Y
7	Mutual Authentication [10], [23],[24],[26],[27]	**N**	**N**	**Y**
8	IP Spoofing [11],[12], [23],[24],[26],[27]	Y	Y	Y
9	Parallel Session Attack [13], [23],[24],[26],[27]	Y	Y	Y
10	Ping Broadcast [14], [23],[24],[26],[27]	Y	Y	Y
11	Password Guessing Attack [15], [23],[24],[26],[27]	Y	Y	Y
12	Server Spoofing [16], [23],[24],[26],[27]	Y	Y	Y
13	Replay Attack [17], [23],[24],[26],[27]	Y	Y	Y
14	Session Hijacking [18], [23],[24],[26],[27]	Y	Y	Y
15	Smart Card Loss Attack [19], [23],[24],[26],[27]	Y	Y	**N**
16	Smurf Attack [20], [23],[24],[26],[27]	Y	Y	Y
17	Stolen Verifier Attack [21], [23],[24],[26],[27]	Y	Y	Y
18	Teardrop Attack [22], [23],[24],[26],[27]	Y	Y	Y

Figure 1: Comparative Analysis of Existing Password Authentication Schemes

After analyzing *Figure 1* it is found that IPAS is required. A Survey is done (*Questionnaire 1*) to find the most acceptable identity authentication parameter by users. From output it is analyzed that finger print would be used as a parameter in hash based scheme for generating IPAS and application of IPAS would enhance TLSP.

This IPAS would use combination of two identity authentication parameters which are password and fingerprint. This IPAS would be able to withstand the above said security requirements and would not be vulnerable to various above stated attacks.


Specification of Attacks and Security Requirements
Analysis of existing Password Authentication Scheme
Comparative Analysis
Need for Generating an Ideal Password Authentication Scheme
Password
Fingerprint
Mutual Authentication and Fortification of Transport Layer Security Protocol

Flow Diagram 1: Generating Ideal Password Authentication Scheme

Now for using finger print as a parameter detailed study of the types of fingerprint and technologies for finger print authentication is required. There are three basic types of fingerprints [29]:

i. **Arches** (It may be plain (ridge enters from one side, make a wave in the center and flow in the opposite side) or tented (angle is there in arch). Delta is not there in arch.
ii. **Loops** (ridge count is there). One core and delta is there in loop.
iii. **Whorls** (Any fingerprint that has two or more delta's is whorl). In it one ridge would be having 2 delta's.

Everyone falls into one of the above said categories. Within these three categories there are thirty different minutiae points. This makes fingerprint unique because no one has the same number of minutiae points on the same place. Following are the technologies for finger print authentication [30]: Correlation (where image itself is used as a template): It is very easy to recreate fingerprint from templates, and which would give access to unauthorized users so it is not safe to use. Texture Descriptors (fingerprint texture is used): captures global and local

features of a fingerprint in a compact fixed length vector which would be finger code. Correlation and Texture Descriptors give access to unauthorized users so third finger print authentication is used in the research proposal which is Minutiae Descriptors. **Minutiae Descriptors** (set of unique features in finger print): Bio hashing is used to replace template based matching (Correlation).

In this research proposal, minutiae descriptors would be used for fingerprint authentication. The motive is to create mathematical abstraction of the minutiae information of the fingerprint so that intruder could not get any relevant information about the original fingerprint. If M is the minutiae point then position(x, y) of M would be required. M could be generated from sensitive fingerprint sensor along with the stated position values. Hash algorithm would be used to generate the hash code of the fingerprint values. In this research proposal new hash algorithm would be generated for conversion of fingerprint values to hash code. There are various hash algorithms which are currently in use for converting fingerprints into hash code but that would not be used in this research proposal. Below mentioned are the existing hash algorithms:

i. **Grid hash algorithm** [30]**:** If there is a situation that partial fingerprints are provided, which means fingerprints are cut to an acceptable limit. So due to this reason grid algorithm is used because it gives matrices of equal sizes for each fingerprint.

ii. **Angle hash algorithm**[30]**:** In this core and delta points are created by putting start of the ridge as core *(cx, cy)* and the point at the divergence of the ridge is delta*(dx, dy)*. This algorithm divides the fingerprint into grid of squares and the number of minutiae in each square is counted and further they are stored in the form of a matrix at the server as hash code. Minutiae points are *M* with specified position *(x,y)*. Now if it is the *ith* minutiae point, then position of the point would be *(xi,yi)*. Join core, delta with the minutiae point and it would take the form of a triangle. Then calculate the slope of the line. Formula for calculating slope of the line is:

$$M1 = y1 - cy / x1 - cx \qquad M2 = y1 - dy / x1 - dx$$

Further calculate the angle for this with the use of following formula:

$$\alpha = tan^{-1} M1 - M2 / 1 + M1.M2$$

And the hash code for the fingerprint would be all the angle calculations:

$(\alpha_1, \alpha_2, \alpha_3, \text{----------}, \alpha_n)$

iii. **Minimum distance hash algorithm**[30]**:** Sometimes it may happen, that only one global feature core or delta could be traced out. In this algorithm a line would be created from minutiae point to the global point (core or delta). Then distance between the both would be calculated. Suppose *M* is the minutiae point with *(xi,yi)* position and *(tx,ty)* if the value of the global point core or delta. Now distance between the *ith* minutiae point and global point would be *di*. The formula for calculating *di* is as follows: $di = sqrt((xi - tx)^2 + (yi - gy)^2)$

Now the minutiae point which would be having the least distance would be core and the process would carry on iteratively. And the algorithm would result in the network of connected line segments. Once this network is generated then by using the property of line segments such as length and the slope of line, hash code would be generated. Any fingerprint with *M* minutiae points would have hash code as:

$(p_1, p_2, p_3, \text{--------}, p_m)$

where *p* is the parameter which is used for hash code.

This research proposal would generate a new hash algorithm (RNA-FINNT) which would work more efficiently, would take less time in calculation and faster than the existing hash algorithms. This new hash algorithm would take finger print as input and hash code as output, the value of which would be stored at the Server. In this research proposal following steps would be used for application of IPAS so that result would be FTLSP (*Figure 2*):

i. Username would be given as input
ii. Password along with finger print would be used for mutual authentication.
iii. Minutiae descriptors would be used for finger print authentication.
iv. New Algorithm RNA-FINNT would be generated for conversion of fingerprint into the hash code. It would result in increased efficiency.

A complete process how to generate an IPAS is explained in *Figure 2*. This IPAS would be applied with the help of a framework and would result in the fortification of TLSP. Complete secure system for transactions would be available if this IPAS is used by the Organizations. RNA-FINNT has resulted quiet beneficial than existing Fingerprint Hash Algorithms. IPAS

has RNA-FINNT implemented in it for fortifying the security at the transport layer. Following are the stated benefits of RNA-FINNT:

i. It has reduced the number of angle calculation,
ii. dependency over the global features is totally removed,
iii. all the grids are executed in parallel so it results in rapid execution or calculation,
iv. error approximation is very less because when the existing fingerprint hash algorithms are used only 8 to 12 minutiae points match is considered for Fingerprint Match but in RNA-FINNT all minutiae points falling in the particular grid are considered for Fingerprint Match. Linear Symmetric Hash function is used with RNA-FINNT for matching the fingerprint values.

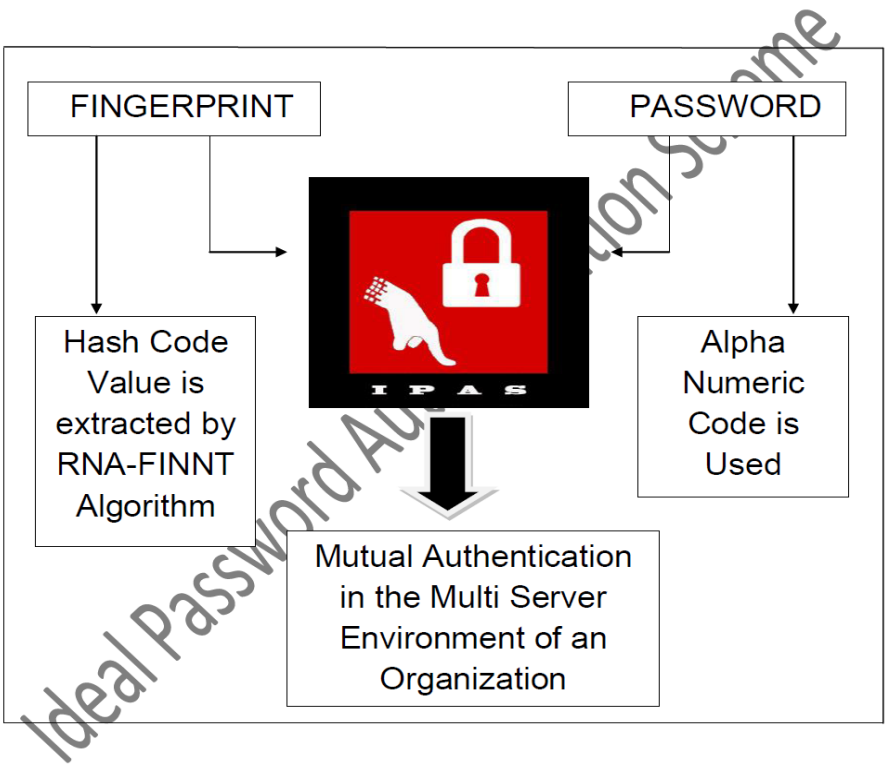

FINGERPRINT
PASSWORD
Hash Code Value is extracted by RNA-FINNT Algorithm
IPAS
Alpha Numeric Code is Used
Mutual Authentication in the Multi Server Environment of an Organization

Figure 2: How an Ideal Password Authentication Scheme is generated

Overall when this IPAS (*Process 1*) would be implemented with the new hash algorithm (RNA-FINNT) then efficiency of the system would improve. And it would result in addition of one more tier to the security protocol (with the use of fingerprint), by which mutual authentication would be very well implemented and further which would fortify the transport layer security protocol.

3. Objectives of Proposal

This research proposal uses Password and Fingerprint as identity authentication parameters. The focus of the proposal is to generate a new fingerprint hash algorithm which if used along with password would form an Ideal Password Authentication Scheme. And when this IPAS is implemented it would result in fortification of transport layer security protocol. This proposal focuses on following objectives:

i. **Deriving a New Fingerprint Hash Algorithm:** RNA-FINNT, a new fingerprint hash algorithm is derived which is efficient than the existing Fingerprint Hash Algorithms.

ii. **Making Fingerprint Match more Authentic than the existing:** Generally in forensic labs 8 to 12 minutiae points are considered to state that fingerprint matches, but the goal of this proposal (with the use of RNA-FINNT) is to consider all the minutiae points falling in each grid so that identity match should be quiet authentic. Dependency over the global features of the fingerprint is totally removed in RNA-FINNT.

iii. **Generating IPAS (with implemented RNA-FINNT) for Security:** Password and Fingerprint assimilation would be done for generating an IPAS. RNA-FINNT would be implemented in this IPAS. This IPAS if used by organizations would help in securing the data or information.

iv. **Implementation of IPAS at Transport Layer for fortifying the Security Protocol:** In order to prove that IPAS (with implemented RNA-FINNT) works efficiently than existing authentication schemes, a framework is designed which would include running flow of this methodology. IPAS would prove (with the help of framework) that transport layer security is enhanced.

v. **Validating Applicability of IPAS (with implemented RNA-FINNT) for Secure Transactions:** If this IPAS is used by the organizations for Online Banking, e-Communication, e-Payments, Identity Authentication etc, it would give efficient results than the existing schemes.

Above stated are the objectives of the proposal. When these objectives would be met an IPAS would be available with implemented RNA-FINNT.

4. Scope of Study

In this research proposal it is very well defined that all the schemes use password or smart cards as the only method of user authentication despite they are vulnerable to various attacks and could not withstand majority security requirements. This research proposal would result in generating an IPAS which would result in FTLSP. Now let us focus on the following scope of study of this research proposal:

i. **Used in Organizations in which identification of the Risks associated with SSL VPN is required** [31]**:** Analysis of the existing password authentication schemes is done so that risks associated with them should be identified. From *Figure 1* it is verified that these are vulnerable to attacks and could not withstand the mentioned security requirements. Because of the risks involved in existing password authentication schemes, SSL VPN is implemented in the organizations. The research proposal is useful for the organizations for identifying the risks associated with implementation of SSL VPN such as Lack of required host security software on public machines, Physical access to shared machines, Keystroke loggers, Endpoints—loss of sensitive information and intellectual property, Man-in-the-middle attacks etc..

ii. **Required in Organizations where Password Authentication is not useful and Accumulation of one more tier to the Security Protocol is needed:** Existing password authentication schemes either use password or smart card for identity authentication. But this research proposal would use fingerprint as a parameter along with the password. This would result in the accumulation of one more tier to the security. As earlier for identity authentication only passwords were used but in this research proposal new IPAS would be generated which would use fingerprint parameter. Implementation of this IPAS in the organizations would result in FTLSP.

iii. **Used to prove the Non vulnerability and withstanding of Ideal Password Authentication Scheme to the defined attacks and security requirements:** As per comparative analysis done in *Figure 1* it is very clear that the existing schemes are vulnerable to attacks and could not withstand all the mentioned

security requirements (RSA: vulnerable to mutual authentication, ElGamal: vulnerable to mutual authentication, Hash based: vulnerable to smart card loss attack). But in IPAS, hash based scheme would be used in which fingerprint along with password parameter would be used. So result of this proposal is IPAS which would be not vulnerable to smart card loss attack, and further it could very well withstand mutual authentication resulting in enhancement of TLSP.

iv. **Used in Organizations which use identity authentication and withstand the Mutual Authentication Security Requirement:** This research proposal focuses to withstand the mutual authentication security requirement? Initially client would provide username to the server which would be unique, server would send fingerprint of one of the finger of client, client would authenticate server by putting same finger on the screen of the system so that it may get match. If it matches authentication of the server is successful. Server would ask for password and another fingerprint of the same client for authentication of the client. If it matches then client authentication is successful. With the use of two parameters password and fingerprint mutual authentication would be successful. So organizations could use IPAS because it withstands mutual authentication

v. **Required to Diminish IP or Server Spoofing:** In IP spoofing normally source address given is incorrect. In such situation an attacker assumes a new identity and any reply generated by the destination would be sent to the attacker. In Server spoofing an attacker pretends to be server to manipulate sensitive data of the legitimate user. Now when mutual authentication is successfully implemented then scope of IP or Server spoofing diminishes. Because the parameters would be stored in the multi-server environment so spoofing becomes a quiet complex. And it is only possible with the implementation of IPAS.

vi. **Used in Organizations where Existing Fingerprint Hash Algorithms are used for identity authentication:** In this research proposal new hash algorithm RNA-FINNT would be generated. In this algorithm fingerprint would be divided into grid of squares and the number of minutiae points in each square is counted. If the number of minutiae points in a specific square of a grid is less than 2 then

the same value would be stored in the matrix which would be the hash code. But if the number of minutiae points in a specific square of a grid is more than 2 then angle calculation would be done. Global feature core or delta would not be included rather one of the minutiae point would act as central point and connection between all the minutiae points in specific square of the grid would be generated. Formula of angle calculation would be used and the output would be stored in the matrix which would be the hash code. So this new hash algorithm would give output as a matrix which would have different values for each square of the grid. And moreover all the squares of the grid would execute parallely which would help in rapid execution. So organizations could successfully implement RNA-FINNT for identity authentication.

vii. **Required in Organizations having Server Side SSL Implemented:** This research proposal would help the organizations in preparing strong IPAS with the use of two parameters password and fingerprint. This would be implemented in one of the existing SSL VPN in multi server environment of any organization. Hashes of user password and fingerprint are often stored in a server database. But in multi server environment username, image and password would be stored at server number 1, hash code of (middle finger and index finger) in server number 2.Collectively mutual authentication would be done in multi server environment. Phishing or Server spoofing would become almost impossible with implementation of IPAS in multi-server environment. So IPAS is required in the organizations which have Server Side SSL implemented.

viii. **Used in Organizations where Multi Server Environment is implemented:** Despite the improvements by SSL, password based authentication protocol does not give satisfactory results. Because an attacker who is able to breach server would be very well able to obtain very large number of user passwords (by Dictionary Attacks). So this research proposal focuses on multi-server environment. An IPAS would be implemented in the organization with multiple server environments because this scheme would have capability of verifying a password, fingerprint which is split among two or more machines. Moreover

number of servers need to collude to recover the password and fingerprint values. An IPAS would be able to accomplish all the goals like:

- password and fingerprint are stored in multi servers and it is not vulnerable to attacks and could withstand security requirements,
- it is efficient and practical and has confidentiality in the communication, even if password could be leaked or stolen, fingerprint values could not be revealed.

So this IPAS would be quiet successful in accomplishing all the above said goals.

ix. **Required in Organizations which deal with Transactions executed at the Transport Layer:** Any organization having SSL implemented, record and handshake protocol would be verified that either the data integrity or security is improved. In this research proposal IPAS would be used with password and fingerprint parameters, which adds one more tier of security to the protocol, so it would overall improve the communication process. New hash algorithm (RNA-FINNT) of the research proposal would result in efficiency and rapid execution. So it would overall result in the FTLSP. Certain measures would also be suggested for mitigation of the risks which may involve in implementing this IPAS. Such measures would generate ideas for future IPAS in a multi-server environment of an organization. This process results in FTLSP.

x. **Scope of research proposal in organizations dealing with e-payments or e-communication etc:** This research proposal states that the main objectives for SSL are authenticating client and server through IPAS (public key encryption would be used to authenticate and hash algorithm would function for generating hash codes), ensuring the data integrity while the transmission at the transport layer (data should not be tampered either intentionally or unintentionally), and securing data privacy while the session is created between client and server after mutual authentication (protection is required from interception, negotiations). All this is an online process so scope of this research proposal is also meant for organizations which deal with e-payments or e-communication etc. Assurance of security is the only requirement of the entire user's, from the organization. For

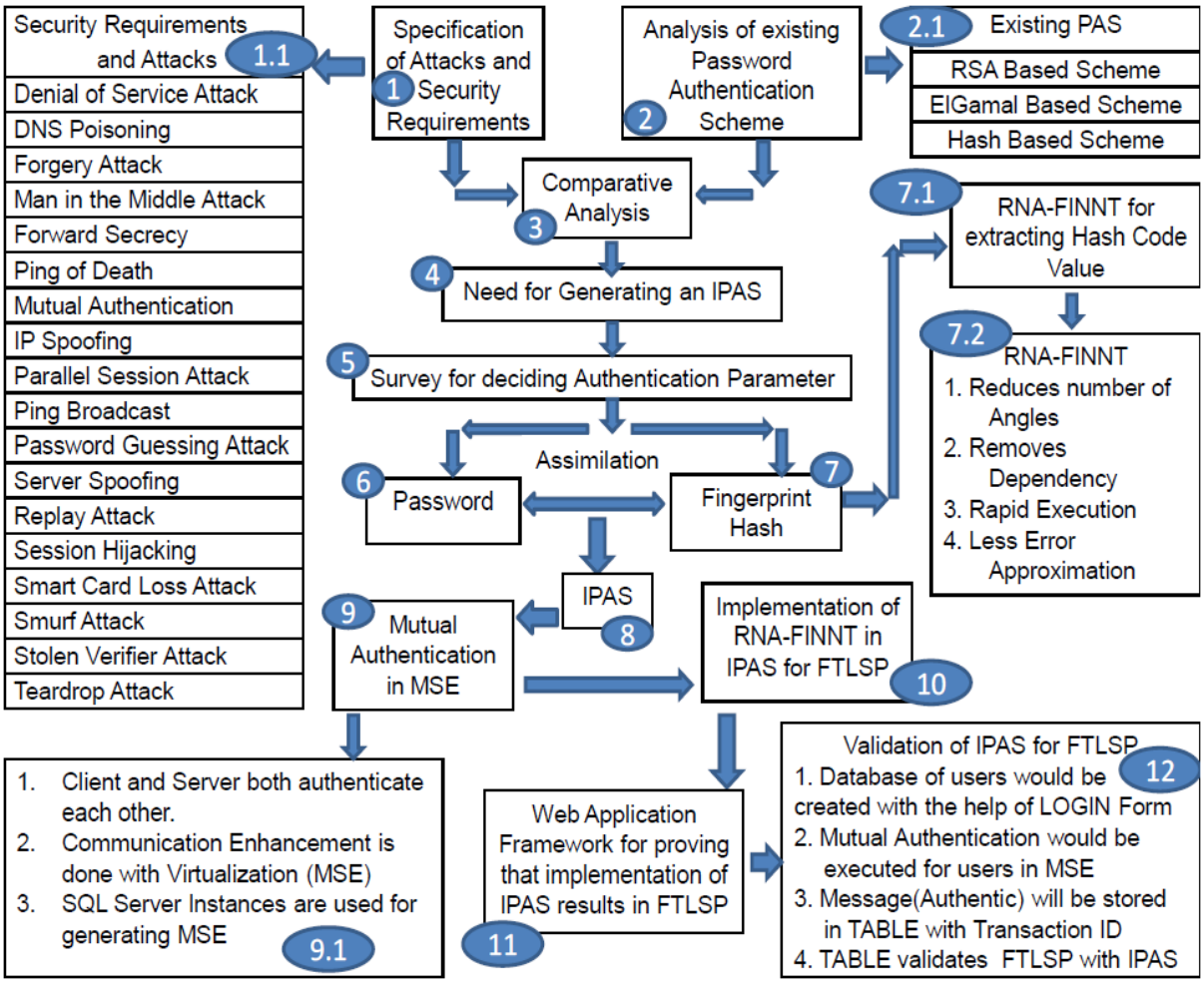
organizations dealing with e-payments and e-communication etc this research proposal proves results in FTLSP by: step wise process for identity authentication (Password and Fingerprint), implementing it in a multi-server environment in order to make possibility of revealing password or fingerprint values almost nil, mutual authentication through values of password and fingerprint for enhancing client and server side security and implementing it with SSL VPN to have additional security.

xi. **Scope of research proposal in organizations where Employees are identified through Identity Authentication Parameters, Password and Fingerprint:** Generally in majority of the organizations employees mark their attendance through biometric machines or they login into the official software of the organization through password**.** So Ideal Password Authentication Scheme (Fingerprint assimilated with the Password) would enhance the identity authentication system. Organizations can implement IPAS into their attendance marking systems or at the login form of the organization official software's so that when any user login's through IPAS then authenticity of the user is proved legitimate. IPAS has RNA-FINNT (New Fingerprint Hash Algorithm) implemented in it, so it will strengthen the security of the data whenever there is transfer of data at the transport layer. Nobody could be able to login maliciously when IPAS would be implemented because IPAS uses the Multi Server Environment in an organization. So scope of the proposal is in all the organizations which make use of identity authentication.

Above mentioned is the scope of study of the research proposal. Proposal results in generation of an Ideal Password Authentication Scheme in which RNA-FINNT (New Fingerprint Hash Algorithm) is implemented. It would result efficient for all the organizations which deal with e-payments, e-communication, online banking, in organizations where employees are identified through Identity Authentication Parameters (Password and Fingerprint), in organizations where enhanced security is required, where data or information flows in bulk etc.

5. Proposed Methodology

User's identity verification or authentication is the key step for data communication, at the transport layer. From the detailed literature review it is identified that existing password authentication schemes are vulnerable to various attacks and they could not withstand majority security requirements. So this research proposal proposes that there is need to generate an IPAS which could secure TLSP from various attacks and result in FTLSP. Following flow or methodology is used in the proposal for proving that IPAS would result in the FTLSP.



Flow Diagram 2: Proposed Methodology for IPAS with RNA-FINNT Implementation

For following this methodology complete process is to be framed. The process would result in generation of an IPAS (*Process 1*) with RNA-FINNT implemented in it.

Now the proposed methodology for generating an IPAS which results in FTLSP is:

1 **Analysis of Existing Password Authentication Schemes:** Complete Analysis of all the existing password-authentication schemes like RSA, ElGamal and Hash Based are to be done. These schemes would be analyzed with algorithm and example so that verification could be done that the schemes support which security requirement and are vulnerable to which attacks. RSA based scheme and ElGamal based scheme could not withstand mutual authentication security requirement but Hash based scheme is vulnerable to smart card loss attack but it can very well withstand the mutual authentication security requirement.

2 **Defining and Comparing the Attacks and Security Requirements:** Definition of all the attacks and security requirements for the existing password authentication schemes would be done. Comparison of all existing password authentication schemes for the defined attacks and security requirements is to be performed. Specifications of attacks and security requirements for IPAS are to be mentioned. According to the literature review done in section 2 it is clearly identified that RSA and ElGamal based scheme both could not withstand mutual authentication security requirement but hash based scheme could withstand but is vulnerable to smart card loss attack. So this research proposal would focus on IPAS which would overcome the problem of smart card loss attack and could withstand mutual authentication security requirement.

3 **Understanding risks associated with SSL VPN:** Complete analysis of the risks associated with SSL VPN with existing password-authentication schemes would be done. Certain risks associated with SSL VPN are Lack of required host security software on public machines, Physical access to shared machines, Keystroke loggers, Endpoints—loss of sensitive information and intellectual property, Man-in-the-middle attacks etc. But certain big organizations like CISCO has identified that security of the data at Transport Layer with SSL could only be possible if security policies and secure access through strong user authentication, host identity verification, host security posture validation, secure desktop, cache cleaning, keystroke logger detection, configuration consideration and user education and security awareness is implemented [1].

Questionnaire

Name: **Gender:** **Age:**

Qualification: **Occupation:** **Place:**

Organization: **Contact No:**

Address: **Email:**

Date: **Signature:**

1. Which among the following is the most common and accepted authentication method for online transactions which you generally use?
   1. Password 2. Smart Card 3.Fingerprint 4. Pass Phrase
2. What do you face as the most concerning challenges in online transactions?
   1. Authentication 2. Security 3.Usability 4. None
3. How secure do you think passwords and tokens are during online transactions?
   1. High 2. Medium 3.Low 4. Not Secure
4. How do you perceive usability of passwords and tokens are during online transactions?
   1. High 2. Medium 3.Low 4. Not Decided
5. Which of these authentication types would you use for online transactions in future?
   1. Fingerprint 2. Iris
   3. Location Based 4. Voice Recognition
6. How do you evaluate security and privacy in online transactions if fingerprint is used as an authentication type?
   1. High 2. Medium 3.Low 4. Not Secure
7. What are your expectations to secure your transactions while using online mode (either for e-purchasing, e-banking or e-communication etc)?
   1. User Authentication 2. Server Authentication
   3. Security from Intruders 4. All of the above
8. Generally you are using password for e-purchasing, e-banking or e-communication etc, but if one more tier of security is added with the use of fingerprint for these transactions to be completely secure than what is the possibility of acceptance for the user?
   1. High 2. Medium 3.Low 4. Not Sure
9. Adding one more tier for enhancing security may result in some additional cost to few users, what is the possibility of acceptance that for enhancing security user can bear the nominal cost?
   1. High 2. Medium 3.Low 4. Not Sure
10. If any prototype could result in complete security for e-purchasing, e-banking or e-communication etc then what is the possibility of user's willingness to purchase that:
    1. High 2. Medium 3.Low 4. Not Sure

Questionnaire 1: Survey for generating an Ideal Password Authentication Scheme

Fortification of TLSP by generating IPAS

4 **Survey for identifying the authentication parameter which is most acceptable by the user's:** It would be on the basis of *Questionnaire 1*.It concludes the following:
This survey has resulted that there is need of generating an IPAS which will result in fortification of transport layer security protocol. Sample area of Punjab was taken which comprised of Universities, Colleges, Banks, Courts and Schools etc. Generally passwords are used by majority of the users for online transactions but for complete security one more tier of security at the transport layer is required. Survey has stated that along with password one more authentication parameter is required. As per majority of the users in future Fingerprint should be used along with the password. Assimilation of fingerprint along with the password will be done to generate an IPAS. This IPAS will be used in all online transactions through a prototype or framework and users are ready to pay nominal cost for purchasing this prototype or framework. Online transactions will be extremely secure with the use of two authentication parameters. Login processes used by majority of the Organizations would become efficient with implementation of IPAS. IP or Server spoofing will almost diminish. And above all this IPAS will result in the fortification of TLSP.

5 **Generating New Hash Algorithm (RNA-FINNT) for producing hash code values of fingerprint:** In this research proposal new hash algorithm RNA-FINNT would be generated which would increase the efficiency of the system, would enhance security at the transport layer, execution of which would be much faster than existing hash algorithms because it results in reduced number of angles and less error approximation. The algorithm would execute in the following manner:

i. Sensor would be used to take fingerprint of the user for first time.
ii. Fingerprint would be divided into grid of squares and the number of minutiae points (M) in each square is counted.
iii. If the number of M < 2 then the same value which would be hash code would be stored in the matrix.
iv. But if M>2 then by picking M at random angle calculation would be done.

v. Global feature core or delta would not be included rather one of the M would act as central point and connection between all the M in specific square of the grid would be generated.

vi. Slope of line would be calculated and formula of angle calculation would be used. Line would be generated between M. One of the M would be (*cx, cy)* and the second M would be *(dx, dy)*. Position of the *M* would be *(x,y)*. Now if it is the *ith* M, then position of the point would be *(xi,yi)*.

Formula for calculating slope of the line is:

$$M1 = y1 - cy / x1 - cx \qquad M2 = y1 - dy / x1 - dx$$

Further calculate the angle for this with the use of following formula:

$$\alpha = tan^{-1} M1 - M2 / 1 + M1.M2$$

And the hash code for the fingerprint would be all the angle calculations:

$$(\alpha_1, \alpha_2, \alpha_3, \text{----------}, \alpha_n)$$

And the output would be stored in the matrix which would be the hash code.

vii. So RNA-FINNT would give output as a matrix which would have different values for each square of the grid. Either the square of the grid would have minutiae count as hash code value or the angle of the M would be hash code.

viii. And moreover all the squares of the grid would execute in parallel which would help in rapid execution.

6 **Generating an Ideal Password Authentication Scheme** (*Process 1*)**:** After comparing the existing password authentication schemes keeping into consideration the attacks and security requirements an IPAS would be generated. Survey proved that Fingerprint is most acceptable identity authentication parameter. So IPAS would have assimilation of Fingerprint and Password (*Process 1*) as resulted from *Questionnaire 1*. Use of fingerprint parameter would add one more tier to the security at the transport layer. Following methodology would be followed to prove authenticity of an IPAS:

i. Hash code value of the password would be stored at the server (database).

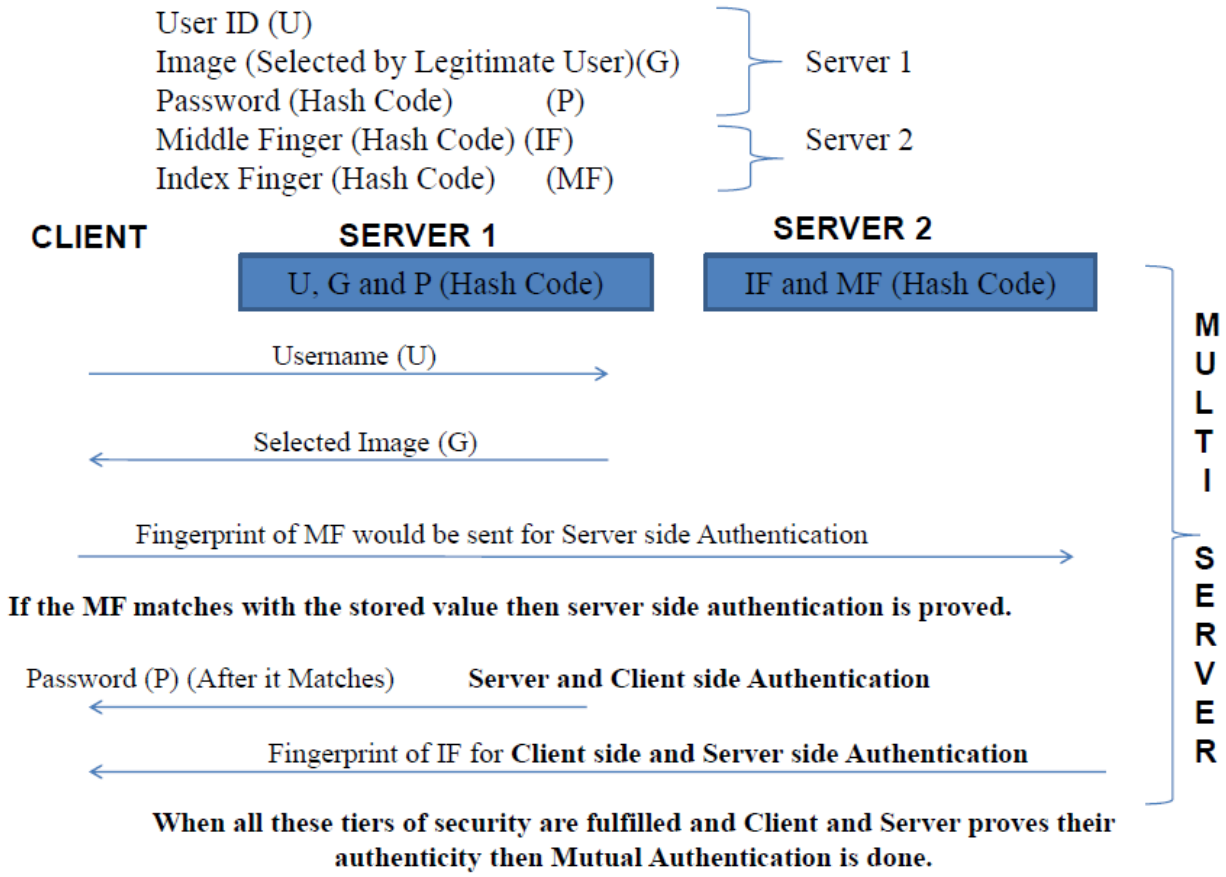
ii. Fingerprint of index finger and middle finger would be taken with the help of sensors like veridicom sensor and optical digital biometrics sensor etc.

iii. Both password and fingerprint would be used for identity authentication of client and server (mutual authentication). So this scheme would withstand mutual authentication security requirement.

iv. Initially organization which is having multi-server environment would store these values on different servers so that phishing could almost diminish.

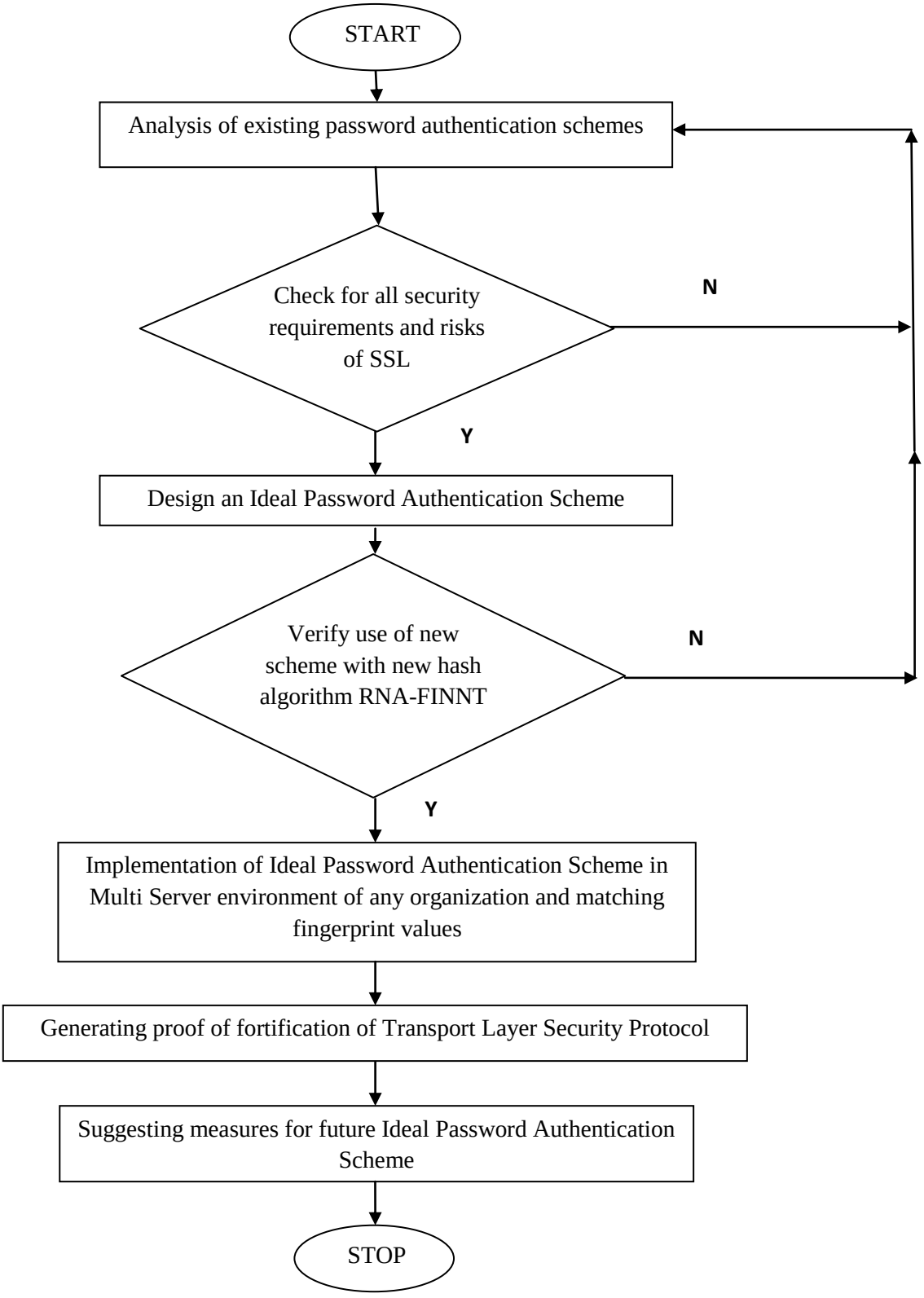
v. Very first time when user would insert these values (password, middle finger fingerprint, index finger fingerprint), it would be stored in the database as shown in *Flow Diagram 3*.

vi. For proving authenticity, this IPAS would be used for mutual authentication. Organizations would use the multi-server environment as follows:


User ID (U)
Image (Selected by Legitimate User)(G)
Password (Hash Code) (P)
Server 1
Middle Finger (Hash Code) (IF)
Index Finger (Hash Code) (MF)
Server 2
CLIENT
SERVER 1
U, G and P (Hash Code)
SERVER 2
IF and MF (Hash Code)
MULTI SERVER
Username (U)
Selected Image (G)
Fingerprint of MF would be sent for Server side Authentication
If the MF matches with the stored value then server side authentication is proved.
Password (P) (After it Matches)
Server and Client side Authentication
Fingerprint of IF for Client side and Server side Authentication
When all these tiers of security are fulfilled and Client and Server proves their authenticity then Mutual Authentication is done.

Flow Diagram 3: Multi Server Environment

IPAS (*Process 1*) would use password and fingerprint which would enhance security as one more tier is added to the security protocol.


START
Analysis of existing password authentication schemes
Check for all security requirements and risks of SSL
N
Y
Design an Ideal Password Authentication Scheme
Verify use of new scheme with new hash algorithm RNA-FINNT
N
Y
Implementation of Ideal Password Authentication Scheme in Multi Server environment of any organization and matching fingerprint values
Generating proof of fortification of Transport Layer Security Protocol
Suggesting measures for future Ideal Password Authentication Scheme
STOP

Flow Diagram 4: Proposed Methodology in Research Proposal

7 **Tremendous use of Ideal Password Authentication Scheme for Identity Authentication:** As per this research proposal IPAS (*Process 1*) would bring ease for proving mutual authentication and could be used by the organizations which make use of identity authentication. Following process would be followed for proving identity in the IPAS:

i. Client would send username to the Server for initial authentication.
ii. Server would send one of the images selected by client and middle finger fingerprint for proving that server is legitimate.
iii. Client verifies the image and put his middle finger on the sensor location at the screen of the system to check either fingerprint matches with the original stored value at the server. If it matches, then authenticity of Server is proved.
iv. Then after validation server would ask for password from the client, if the filled password matches with the original stored value at the server then server demands for index finger fingerprint. Client puts his index finger on the sensor location at the screen of the system, if the fingerprint matches then client's authentication is done. In this way it results in mutual authentication.
v. Finally this will end up with the completion of login process. Mutual authentication with this IPAS would result in FTLSP.

8 **Matching of password and fingerprint with the values stored at server for identity authentication:** There may be a possibility that when authenticity is to be proved then fingerprint could not match because every time client could not place the finger at the same location and in the same way. So when RNA-FINNT would execute it would definitely generate a different hash code value every time. For this following process would be followed so that authenticity process could be enhanced:

i. Initial hash values of password and fingerprint are already stored at the server.
ii. Password is always the same fixed input so every time when client would insert password then hash algorithm would generate same hash code output.
iii. For fingerprint every time same fixed input could not be given because client could not place finger in the same way and location as it was done initially.

iv. When fingerprint is given as input, RNA-FINNT would execute and output *Z*.

v. Now this *Z* is not going to match with the original stored value at the server.

vi. Linear symmetric hash function (LSHF) would run and generate value *Y* [32].

LSHF would execute: Suppose that two fingerprints originating from one finger differ by scale and rotation. If M are represented on a complex plane, then scaling and rotation can be expressed by function: $f(z) = rz + t$

Let $(c_1, c_2, c_3, \ldots\ldots, c_n)$ be the set of M of index finger (first time) and $(c_1', c_2', c_3', \ldots\ldots, c_n')$ be the set of M of index finger (second time) then transformation would be done with function $f(z) = rz + t$

such that $c_i' = f(c_i') = r(c_i') + t$ *where* $i = 1,2,3,\ldots\ldots,n$

Functions for minutiae positions would be:

$h_1(c_1, c_2, c_3, \ldots\ldots, c_n) = (c_1, c_2, c_3, \ldots\ldots, c_n)$

$h_2(c_1, c_2, c_3, \ldots\ldots, c_n) = (c_1^2, c_2^2, c_3^2, \ldots\ldots, c_n^2)$

……

$h_m(c_1, c_2, c_3, \ldots\ldots, c_n) = (c_1^m, c_2^m, c_3^m, \ldots\ldots, c_n^m)$

This hash function would work in linear symmetric way so the result would be generated symmetrically. When *r* and *t* are found then higher order hash functions could be used to check it the fingerprints match. Then the function would result as follows: $h_3' = r^3h_3 + 3r^2th_2 + 3rt^2h_1 + nt^3$

For checking either the results match or not following steps will run [32] [33]:

- At the time of enrollment M are extracted and *K* symmetric hash functions are evaluated.
- The result after enrollment is stored in the server (database).
- In order to match again M are extracted, *K* symmetric hash functions are evaluated and passed to server for matching.
- By using values of first two hash functions the transformation parameters *r* and *t* would be found.
- Remaining K-2 hash functions values would be used to verify that minutiae set is matching or not.

vii. Y generated would match with the initially stored value if it is a legal user.

So LSHF is used to verify either the client is legal or not. And this function executes in the process of mutual authentication with the help of two identity authentication parameters password and fingerprints. Transformation is used in the LSHF.

9 **Usage of SQL Server Instances for creating Virtual Multi Server Environment:** From the above mentioned methodology an IPAS would be generated and further it would be implemented in one of the existing SSL VPN in multi-server environment of any organization. Reason of implementation in the multi-server environment is that, different servers would be used to store different parameter values as mentioned on *Flow Diagram 3,* it would almost diminish the process of phishing. Expected output would be that IP or Server spoofing would become almost impossible and security would be enhanced. Objectives are very clear that IPAS is gratifying the multi-server environment [34]. Moreover client is most concerned about security of payments or data integrity and communication, so if the process of authentication would have tiers and parameters are stored at different servers then it would enhance the security protocol. Install first instance of the SQL Server in one of the hard drive of system and install second instance of SQL Server in the another hard drive of same system [35]. Same OS would be used for both instances. So no issue about compatibility would arise. With the Linked Servers both the instances would be linked. This would generate a multi server environment with the help of two instances in the same system [36]. IP address specifications and TCP Port that accepts the connection are required for integrating servers. Simulator would discover the IP addresses on the local machine. Particular IP address would be selected and one of the protocol buttons would be clicked to add virtual server [37].

Following features are specific requirement for multi server environment [38] [39]:

- Name and TCP Port for each Server
- Servers could be created and deleted and log entry is required
- Intervals for each client could be set in the simulator

Testing and Validation of this IPAS would be done on this simulator (which would be created in the form of a Website). This simulator would generate the proof of mutual

authentication which would show the evidence of tiers added to the security protocol. So IPAS proposed here would make e-payments and e-communication more secure.

10 **Proof for Resourcefulness of IPAS (Applicability is shown by deriving proof of fortification of TLSP with implementation of IPAS):** With the implementation of IPAS in multi-server environment of any Organization, the proof would be generated that transport layer is fortified. When TLSP is fortified the proof for resourcefulness of IPAS is generated. This IPAS would not be vulnerable to attacks and would be able to withstand the security requirements. When the security requirements are fulfilled then transmission or communication results in data integrity and security which would further result in the enhancement of Record Protocol and Handshake Protocol of SSL. When both the protocols of SSL are enhanced then it would ultimately result in the fortification of TLSP. The major security requirements which this IPAS would fulfill are [40][41]:

i. **Confidentiality** (Protection from disclosure to unauthorized persons)
ii. **Integrity** (Assurance that information has not been modified unauthorizedly)
iii. **Authentication** (Assurance of identity of originator of information)
iv. **Non-Repudiation** (Originator cannot deny sending message)
v. **Availability** (Not able to use system or communicate when desired)
vi. **Anonymity** (For evaluation of instructors)
vii. **Traffic Analysis** (Sender and Receiver should not know their identity)

This research proposal states that IPAS in which RNA-FINNT is implemented is quiet resourceful. For deriving the proof framework is designed to show the fortification of TLSP. Fortification of TLSP is the application part of IPAS in which RNA-FINNT is implemented. Application of IPAS at the transport layer visualizes the following benefits which far sure make the communication process at the transport layer more secure:

i. Two parameters are used in the IPAS to enhance security.
ii. This IPAS would withstand mutual authentication security requirement.
iii. Login process would be complete after proving authenticity in three phases so intruders could fail at one or another step.

iv. IP or Server spoofing is not possible with the implementation of IPAS.

v. In RNA-FINNT global point's core or delta are not considered so it results in the reduced number of angles.

vi. Hash code matrix would comprise of values of count of M in a specific square of the grid and angle calculated hash code for some squares of the grid, which would make matrix of hash code more secure.

vii. All the squares of grid run in parallel so execution of RNA-FINNT is faster.

viii. As the matrix is having secure hash code so the chance of increase in the error is not there, rather chance of error reduction could be visualized as identity authentication runs in steps. Number of angles is reduced for calculation; all squares of the grid run in parallel, mutual authentication is done so adding more tiers to the security protocol enhances the process of security.

This IPAS executed with RNA-FINNT would overall result in the FTLSP.

11 **Web Application Framework for implementation of IPAS for Proving the Proficiency of IPAS (Transport Layer would be Fortified):** A Framework would be created with the help of ASP.Net and SQL Server which would generate a multi server environment as shown in *Flow Diagram 3*. This framework would authenticate the proficiency of IPAS. This is to show the application part of IPAS so that organizations could understand the process of flow of IPAS. The following steps would be followed to validate the results:

i. A Website would be created with the help of ASP.Net and database with the use of SQL Server.

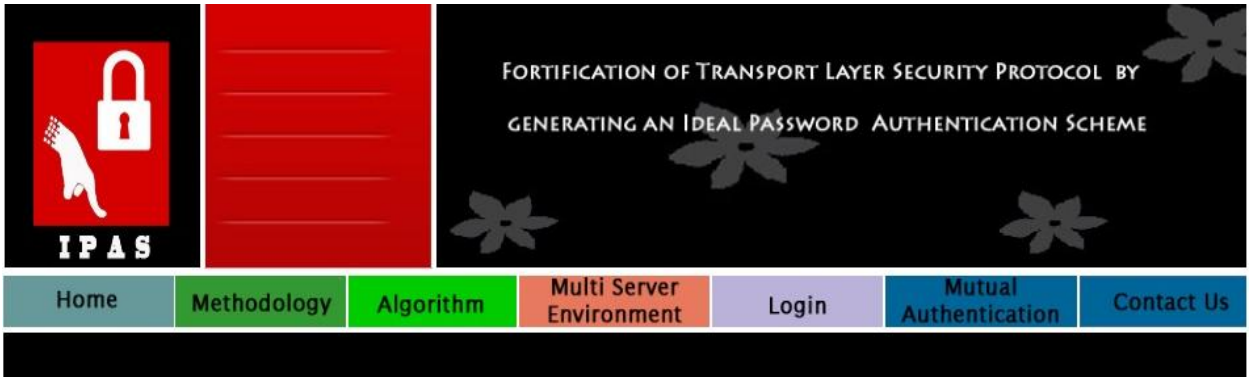


Figure 3: Layout of the Framework

The tabs included in the website are Home, Methodology, Algorithm, MSE, Login Form, Mutual Authentication Form and Contact Us. Logo of the website comprises of combination of Password and Fingerprint both.

This layout of the framework (*Figure 3*), is designed to generate IPAS resulting in FTLSP.

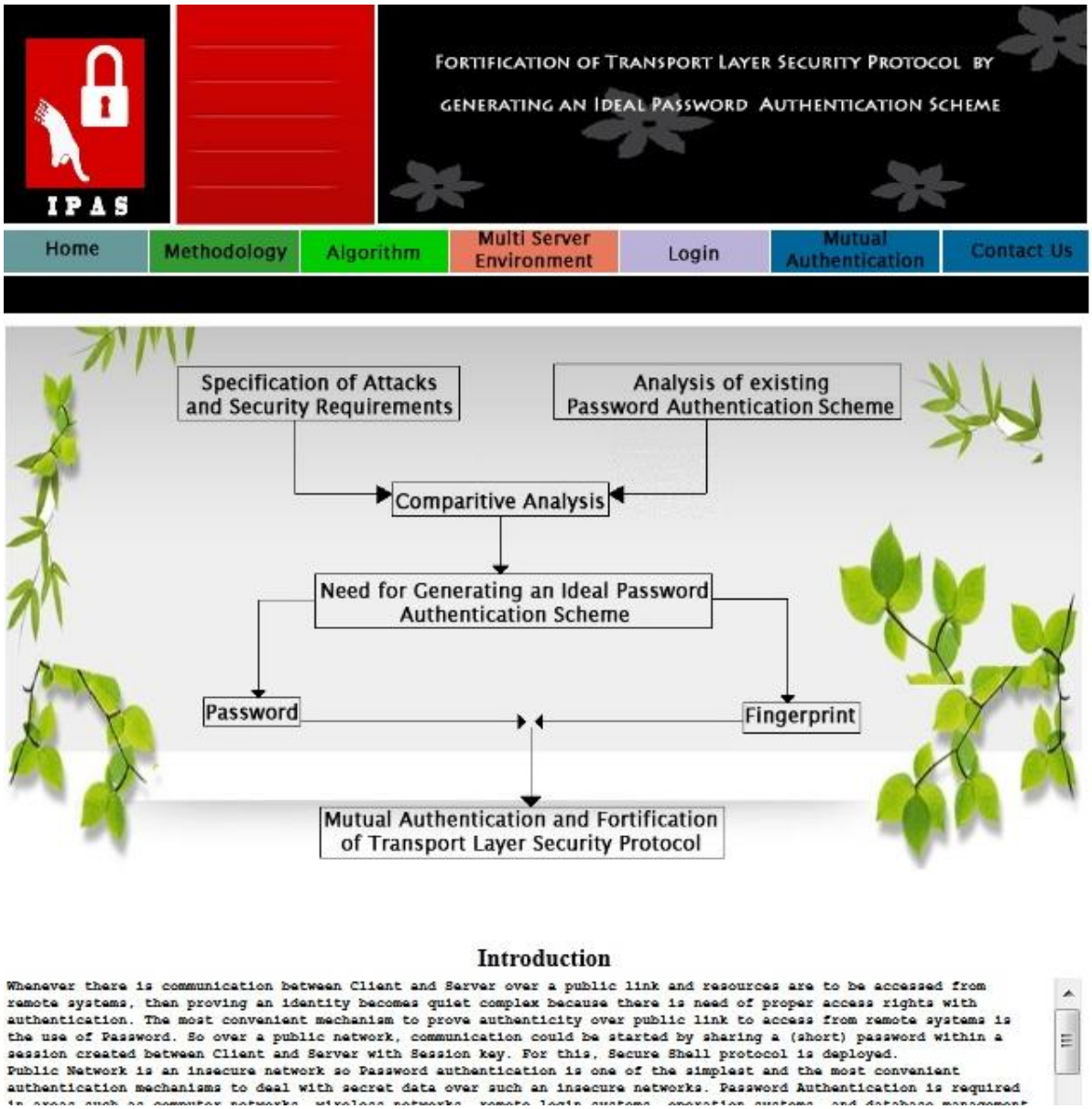

IPAS
FORTIFICATION OF TRANSPORT LAYER SECURITY PROTOCOL BY GENERATING AN IDEAL PASSWORD AUTHENTICATION SCHEME
Home
Methodology
Algorithm
Multi Server Environment
Login
Mutual Authentication
Contact Us
Specification of Attacks and Security Requirements
Analysis of existing Password Authentication Scheme
Comparitive Analysis
Need for Generating an Ideal Password Authentication Scheme
Password
Fingerprint
Mutual Authentication and Fortification of Transport Layer Security Protocol
Introduction
Whenever there is communication between Client and Server over a public link and resources are to be accessed from remote systems, then proving an identity becomes quiet complex because there is need of proper access rights with authentication. The most convenient mechanism to prove authenticity over public link to access from remote systems is the use of Password. So over a public network, communication could be started by sharing a (short) password within a session created between Client and Server with Session key. For this, Secure Shell protocol is deployed.
Public Network is an insecure network so Password authentication is one of the simplest and the most convenient authentication mechanisms to deal with secret data over such an insecure networks. Password Authentication is required

Figure 4: Layout of the Home Page

ii. Home tab would comprise of flowchart which would give details of attacks and security requirements, existing password authentication schemes, comparison of all existing password authentication scheme, need of

generation of IPAS, mutual authentication, combination of Password and Fingerprint for generating an IPAS and proof of FTLSP. Clicking on the above said links of the flowchart would give details of all the parts of the flowchart as mentioned in the above statement (*Figure 4*). Link of published research paper is given at the top of the website (*Figure 4*)

Complete introduction of all the parts of the flowchart are given on the Home page in details.

iii. Methodology tab would define the detailed proposed methodology for the research proposal as mentioned in the Section of Proposed Methodology along with Flowchart. Link of published research paper of it is given at the top of the website along with Logo and Title of the Website.

iv. Algorithm tab would display the flowchart of the algorithm RNA-FINNT which defines the benefits which Reduced Number of Angles Fingerprint Hash Algorithm gives. IPAS would be implemented with RNA-FINNT.

Complete detail of the algorithm along with benefits when implemented in the public network increases the efficiency of the system. Algorithm results in reduced number of angles.

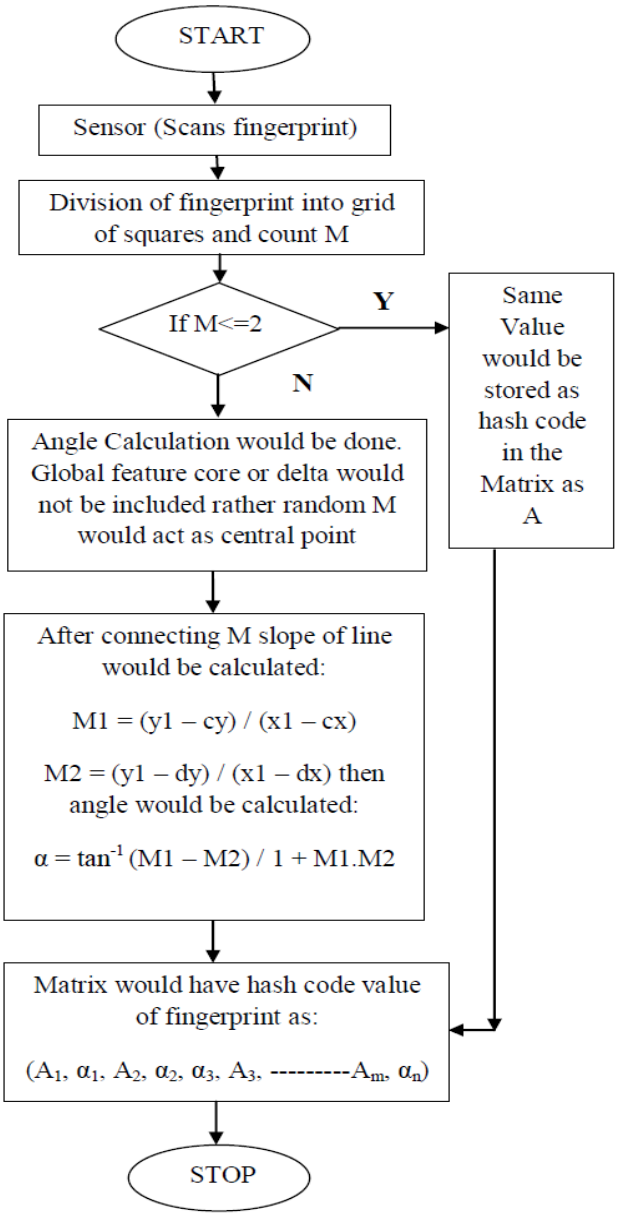

START
Sensor (Scans fingerprint)
Division of fingerprint into grid of squares and count M
If M<=2
Y
N
Same Value would be stored as hash code in the Matrix as A
Angle Calculation would be done. Global feature core or delta would not be included rather random M would act as central point
After connecting M slope of line would be calculated:
M1 = (y1 – cy) / (x1 – cx)
M2 = (y1 – dy) / (x1 – dx) then angle would be calculated:
α = tan-1 (M1 – M2) / 1 + M1.M2
Matrix would have hash code value of fingerprint as:
(A1, α1, A2, α2, α3, A3, ---------Am, αn)
STOP

Figure 5: Layout of the Algorithm

v. Login form tab is there which would ask user for initial input values which are username, image of the choice of user, password, fingerprint of index and middle finger. Below mentioned is the Login Form (*Figure 6*).Initial values would be stored in SQL Server as mentioned in *Flow Diagram 3*.

vi. Database would be created in SQL Server which would store initial input of the Username, Image (Selected by the User), Password and hashed finger print values of Index and Middle finger of the legitimate user.

vii. When initial input would be sent to the database new generated hash algorithm would save the hashed finger print values to the created database. So the database would have username stored in the text format, image only jpeg format, password in hashed code and index and middle finger fingerprints in the hashed code format.

viii. Mutual Authentication form tab checks for the implementation part. When the process of mutual authentication has to be done then steps of *Flow Diagram 3* mentioned below would be followed. Above mentioned is the form.(*Figure 7*)

Following steps would be followed in mutual authentication as in Flow Diagram 3:

i. STEP 1 Client would send User Name, Server would send selected image to the client.

ii. STEP 2 Client would check the image and put fingerprint of middle finger for Server side authentication. If the middle fingerprint matches with the stored value then server side authentication is proved.

iii. STEP 3 Server would ask for Password, if it is correct then server would ask for fingerprint of Index finger for Client side Authentication.

iv. STEP 4 when all these tiers of security are fulfilled and Client and Server prove their authenticity then Mutual Authentication is done.

ix. Contact Us tab gives details of contact for the successful implementers of the website which is in the form of Simulator.

It will result in data integrity and security, which strengthens record and handshake protocol of SSL. Enhancement of SSL would result in fortification of the Transport Layer Security Protocol. This proves the resourcefulness of IPAS in which RNA-FINNT is implemented.

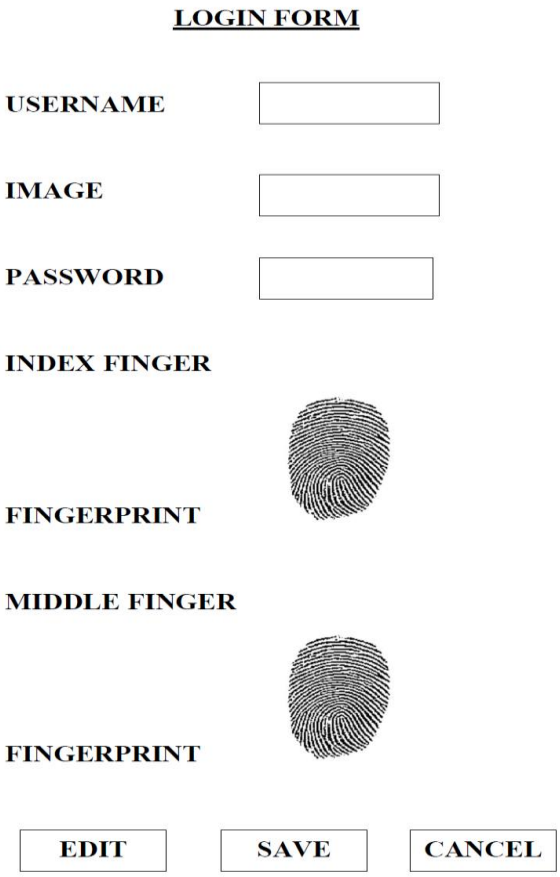


Figure 5: Login Form

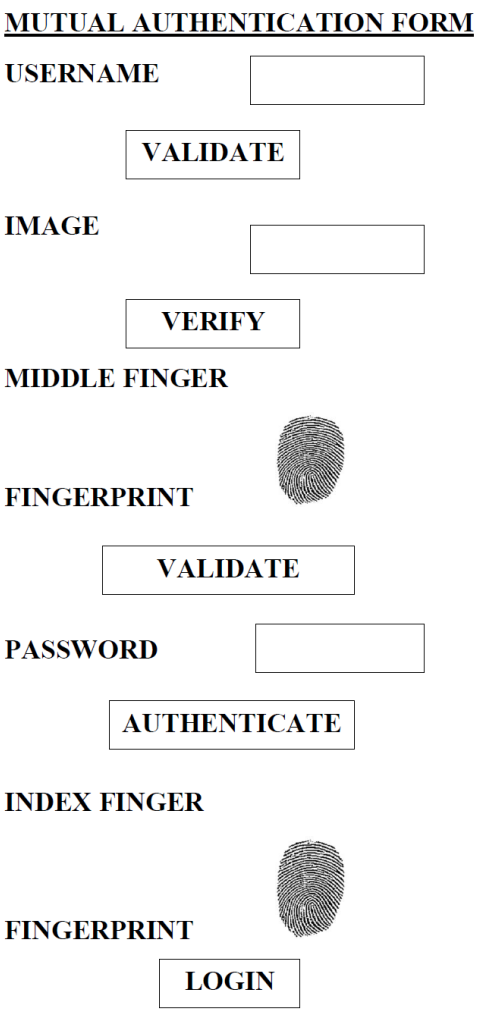


Figure 6: Mutual Authentication Form

12 **Validation of Results for Applied IPAS in the Web Application Framework:** The data of 100 individuals would be collected through the Login Form (*Figure 6*). Entries would be stored in the tables in different instances of the SQL Server (*Flow Diagram 3*). Identification of the user would be done through Mutual Authentication Form (*Figure 7*). If the execution of the form is done properly then Valid Authentication message would be stored in the New Table in the SQL Server along with the Transaction ID of the user. This New Table would validate the results of applied IPAS in which RNA-FINNT is implemented for fingerprint values.

While using this framework analyzed Survey is completely kept in mind. And IPAS is generated on the basis of the output of the Survey only.

Survey discussed above (*Point iv of Proposed Methodology*) is done in the Sample Area. Survey is conducted on the Client Side for the feasibility that either user is ready to bear the additional cost for the device required for extracting the fingerprint value and ready for additional procedural burden. Survey focuses, that either Pass Phrase would be preferred rather than Password or not. Overall analysis of the Survey on the basis of Choice of the user, on the basis of Gender and on the basis of age is as follows and IPAS is generated keeping in mind the output of the Survey:

i. Password is the most common and accepted authentication method for online transactions which is generally used by the users.
ii. Security is the most concerning challenges in online transactions.
iii. Passwords and Tokens have medium security during online transactions.
iv. Users perceive usability of passwords and tokens at medium level during online transactions.
v. In future users would prefer fingerprint as authentication parameter.
vi. Security and privacy would be at highest level if fingerprint is used as an authentication type.
vii. User authentication, Server authentication and security from intruders are expected by majority of the users for secure transactions while using online mode either for e-purchasing, e-banking or e-communication etc.
viii. If fingerprint is used as the authentication parameter in online transactions then possibility of acceptance of data being completely secure is very high.
ix. Possibility of acceptance to bear that nominal cost for enhancement of the security is at medium level by the users.
x. Any prototype which results in complete security for e-purchasing, e-banking etc then the possibility of user's willingness to purchase that is at maximum. Users can bear additional cost for getting complete security in online transactions.

Because Survey resulted in the need of generating an IPAS so this framework is designed to show the application part of the IPAS. This framework is applied at the login process of any software or online transactions and would enhance the security. This framework for IPAS in which RNA-FINNT is implemented results in fortification of TLSP.

13 **Suggestive Measures for future Ideal Password Authentication Scheme:** While verifying the goal accomplishment of the IPAS there are certain constraints in meeting goals of all the security requirements [42]. IPAS claims [43]:

- to fulfill all the specified goals and not to be vulnerable to attacks
- to include two parameters to add more security
- to a generate new hash algorithm for efficiency and faster execution
- for mutual authentication and to withstand security requirements
- to fortify the transport layer security protocol

But certain constraints may exist while executing the process. Flow of process need to be sequential as mentioned above and no variation is allowed in the stated methodology. So all the constraints are to be mentioned when and where they exist and measures are to be suggested for mitigation upon the risks involved in implementation of the IPAS.

Above stated is the proposed methodology which if executed properly would surely enhance security, would make e-payments or e-communication more authentic. Organizations which have multi-server environment could successfully implement this IPAS. With the above said methodology IPAS would be generated which would have two parameters which are password and fingerprint to add more tiers to the security:

- would fulfill above mentioned security requirements,
- would accomplish all the specified goals for ideal password authentication scheme,
- would not be vulnerable to attacks,
- would generate new hash algorithm RNA-FINNT which would have more efficiency than existing algorithms,
- faster execution and more secure than existing hash algorithms,
- would result in more security for e-payments or e-communication,
- would result in diminishing the possibility of phishing, IP Spoofing and Server Spoofing.

So overall it would result in data integrity and security which would enhance record and handshake protocol of SSL. Enhancement of both the protocols would result in the fortification of transport layer security protocol. This complete enhancement is the application of generated IPAS in which RNA-FINNT is implemented.

6. References

1. E. Bresson, O. Chevassut, and D. Pointcheval," Security Proofs for an Efficient Password-Based Key Exchange," in 10th ACM Conference on Computer and Communications Security, pp. 1-2,October 27, 2003, Washington, DC, USA.
2. Peter Buhler, Thomas Eirich, Michael Steiner and Michael Waidner," Secure Password-Based Cipher Suite for TLS", in Network and Distributed Systems Security Symposium(NDSS 2000),San Diego, California, February 2000.
3. "SSL VPN Security," http://www.cisco.com/web/about/security/intelligence/05_08_SSL-VPN-Security.html
4. Craig A. Huegen, "Network-Based Denial of Service Attacks," www.pentics.net/denial-of-service/presentations/.../19980209_dos.pp...
5. Kim Davis," DNS Cache Poisoning Vulnerability Explanation and Remedies," www.iana.org/about/.../davies-viareggio-entropyvuln-081002.pdf,Viareggio Italy October 2008,
6. David A. McGrew and Scott R. Fluhrer ,"Multiple forgery attacks against Message Authentication Codes," eprint.iacr.org/2005/161.pdf ,Cisco Systems, Inc., May 31, 2005
7. Alberto Ornaghi, Marco Valleri ,"Man In the Middle Attacks Demos," in BlackHat Conference, USA 2003
8. DongGook Park, Colin Boyd and Sang-Jae Moon ,"Forward Secrecy and Its application to Future Mobile Communications Security," www.dgpark6.com/Down/pkc2000_FwdSec.pdf
9. Renaud Bidou,"Ping Of Death," www.iv2-technologies.com/DOSAttacks.pdf
10. "Mutual Authentication," en.wikipedia.org/wiki/Mutual_authentication
11. "IP Spoofing,"www.sans.org/reading.../introduction-ip-spoofing_959, United States, SANS
12. Christoph Hofer, Rafael Wampfler,"IP Spoofing," rvs.unibe.ch/teaching /cn%20applets/IP_Spoofing/IP%20Spoofing.pdf

13. Alec Yasinsac, Sachin Goregaoker," An Intrusion Detection System for Security Protocol Traffic," Department of Computer Science, Florida State University,p-12,1996
14. "Ping Broadcast,"en.wikipedia.org/wiki/Broadcast_radiation
15. Vipul Goyal, Virendra Kumar, Mayank Singh, Ajith Abraham and Sugata Sanyal ," CompChall: Addressing Password Guessing Attacks," http://eprint.iacr.org /2004/136.pdf , 2003
16. Larry Seltzer ,"Spoofing Server-Server Communication: How You Can Prevent It," www.verisign.com/ssl/ssl.../ssl.../whitepaper-ev-prevent-spoofing.pdf ,2009
17. Alec Yasinsac, Sachin Goregaoker," An Intrusion Detection System for Security Protocol Traffic," Department of Computer Science, Florida State University,p-12,1996
18. Shray Kapoor ,"Session Hijacking Exploiting TCP, UDP and HTTP Sessions," infosecwriters.com/text_resources/.../SKapoor_SessionHijacking.pdf
19. Rajaram Ramasamy, Amutha Prabakar Muniyandi ,"New Remote Mutual Authentication Scheme using Smart Cards," Transactions on Data Privacy ,Volume 2, p-141—152,2009
20. "Smurf Attack," http://en.wikipedia.org/wiki/Smurf_attack
21. Hanjae Jeong, Dongho Won and Seungjoo Kim ,"Weaknesses and Improvement of Secure Hash-Based Strong-Password Authentication Protocol," Information Security Group, Journal Of Information Science and Engineering 26, 1845-1858 (2010)
22. "Teardrop Attack Detection," https://www.daxnetworks.com/Dax/Products /Switch/DTS_T5C_24G_24GT.htm
23. Tom Davis," RSA Encryption," http://www.geometer.org/mathcircles,2003
24. Brent Waters, Allison Bishop, El Gamal Encryption CS395T Advanced Cryptography, Lecture 3,27th January 2009
25. "ElGamal Encryption," www.informatics.indiana.edu/markus/i400/ lecture7.ppt
26. Kumar Mangipudi and Rajendra Katti,"A Hash-based Strong Password Authentication Protocol with User Anonymity," International Journal of Network Security, Vol.2, No.3, PP.205–209, May 2006 (http://isrc.nchu.edu.tw/ijns/)

27. Hanjae Jeong, Dongho Won and Seungjoo Kim ,"Weaknesses and Improvement of Secure Hash-Based Strong-Password Authentication Protocol," Information Security Group, Journal Of Information Science and Engineering 26, 1845-1858 (2010)
28. "Example of Hash Based Scheme," http://www.cacr.math.uwaterloo.ca/hac/
29. "Basic Types of fingerprints," http://www.odec.ca/projects/2004/fren4j0/public_html/fingerprint_patterns.htm
30. Sahil Goyal and Mayank Goyal," Generation of hash functions from fingerprint scans," Indian Institute of Technology Guwahati, October 2011
31. "SSL VPN Security," http://www.cisco.com/web/about/security/intelligence/05_08_SSL-VPN-Security.html
32. "Symmetric hash functions for fingerprint minutiae," http://www.biometrics.org/bc2004/Presentations/Conference/.../Sergey.pdf
33. Atsushi Sugiura, Yoshiyuki Koseki, " A User Interface Using Fingerprint Recognition- Holding commands and Data Objects on Fingers-,"C & C Media Research Laboratories, NEC Corporation, Japan 1998.
34. Raffaele Cappelli, Dario Maio, Davide Maltoni, James L. Wayman, Anil K. Jain," IEEE Transactions on Pattern Analysis and Machine Learning, Vol.28,No.1,January 2006.
35. Qijun Zhao, Lei Zhang, David Zhang, Nan Luo, " Direct Pore Matching for Fingerprint Recognition", Biometrics Research Center, Hong Kong 2009.
36. Le Hoang Thai, Ha Nhat Tam," Fingerprint Recognition using Standardized Fingerprint Model", International Journal of Computer Science Issues, Vol.7, Issue 3, No.7, May 2010.
37. Jianjiang Feng, Jie Zhou," A Performance Evaluation of Fingerprint Minutiae Descriptors", IEEE 2011.
38. Anil K. Jain, Jianjiang Feng," Latent Fingerprint Maching", IEEE Transactions on Pattern Analysis and Machine Intelligence, Vol.33, No.1, January 2011.
39. "Multi Server Simulator for Network Testing," http://www.paessler.com/serversimulator

40. “Transport Layer Security (Protect Sensitive Data- and Comply with regulations-with TLS/SSL ”, http://www.techsoup.org/learningcenter/networks/page11959.cfm
41. “Implementing Transport and Message Layer Security-Microsoft Patterns and Practices”, http://msdn.microsoft.com/en-us/library/ff647370
42. Chin-Chen Chang,Chih-Chiang Tsou,Yung-Chen-Chou,” A remediable image authentication scheme based on feature extraction and clustered VQ,” PCM'07 Proceedings of the multimedia 8th Pacific Rim conference on Advances in multimedia information processing, 2007(http://dl.acm.org/citation.cfm?id=1779525)
43. Gerard Blokdijk,” Password Management: High-impact Strategies - What You Need to Know: Definitions, Adoptions, Impact, Benefits, Maturity, Vendors”, 2011 (http://www.scribd.com/doc/61409165/Password-Management-High-impact-Strategies-What-You-Need-to-Know-Definitions-Adoptions-Impact-Benefits-Maturity-Vendors)